

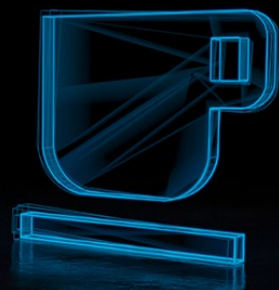


THE
TECHNOLOGY
PROVIDER

FORTIOS 7.2 NEUE FEATURES

ALSO & FORTINET

Tech & Snack



Andreas Tischer, Fortinet
Martin Ruesch, ALSO Schweiz AG
Chris Tanasic, ALSO Schweiz AG

21. Juni 2022

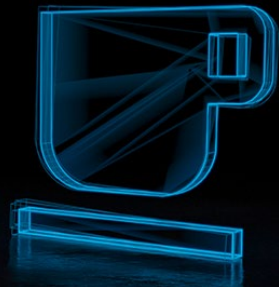




WILLKOMMEN BEI TECH & SNACK, TEIL 2 😊

ALSO & FORTINET

Tech & Snack



WER **WIR** SIND



**Andreas (Andi)
Tischer**

Channel PreSales Engineer
Fortinet



**Martin (Tinu)
Ruesch**

Tech. Consultant Security
ALSO Schweiz



**Cvijetin (Chris)
Tanasic**

Tech. Consultant Security
ALSO Schweiz

AGENDA

- ▶ **Was gibt es Neues?**
 - ▶ **Neue FortiGate Releases**
 - ▶ **FortiCare – Was ist neu?**
- ▶ **Topic: FortiOS 7.2 – Neue Features inkl. Demo**
- ▶ **Q & A**



HOUSEKEEPING RULES



Das Webinar wird aufgezeichnet!



MS Teams Chat für Fragen verwenden



Slides werden nachträglich verschickt



Fragebogen/Survey ausfüllen

MUESLI-BECHER VON MYMUESLI.CH

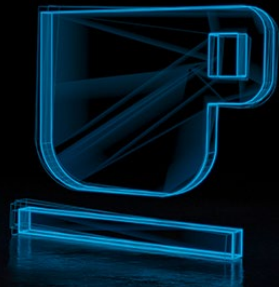




FORTIGATE – NEUE MODELLE

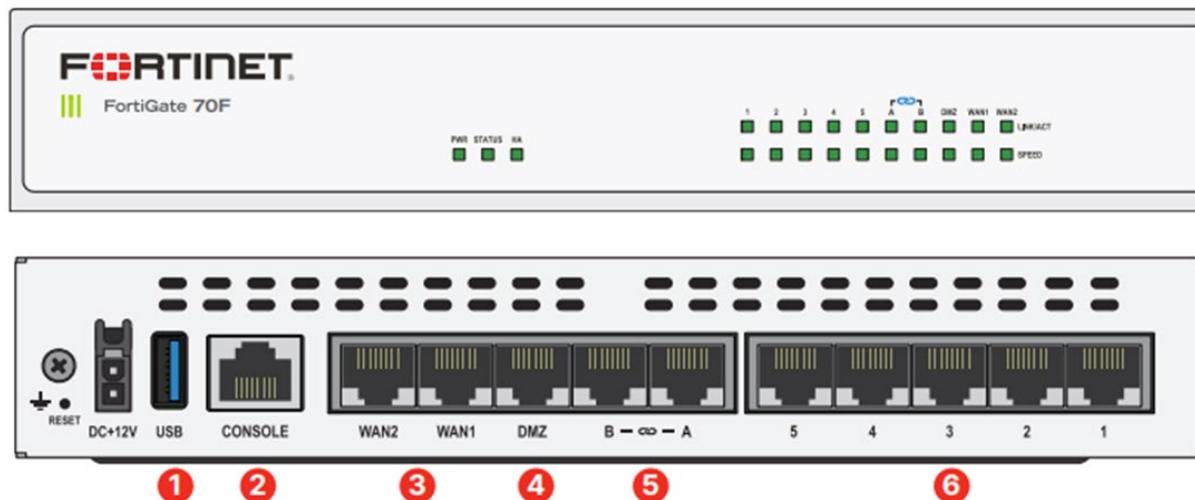
ALSO & FORTINET

Tech & Snack



FORTIGATE 70F

FortiGate 70F/ 71F



Interfaces

1. 1x USB Port
2. 1x Console Port
3. 2x GE RJ45 WAN Ports
4. 1x GE RJ45 DMZ Port
5. 2x GE RJ45 FortiLink Ports
6. 5x GE RJ45 Internal Ports

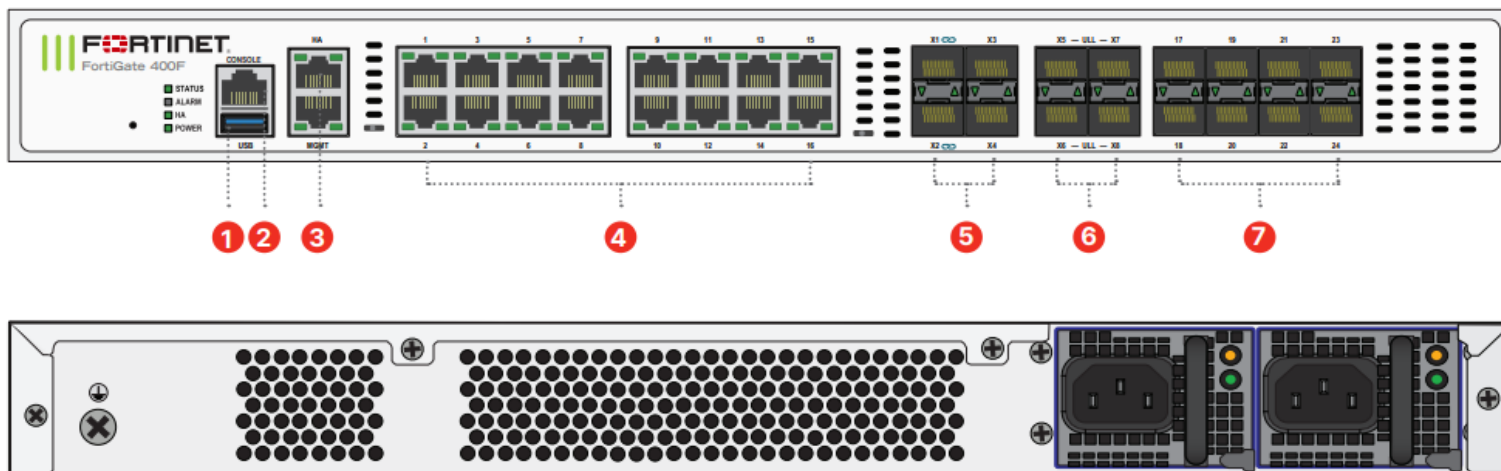
Hardware Features



Firewall	IPS	NGFW	Threat Protection*
10 Gbps	1.4 Gbps	1 Gbps	800 Mbps

FORTIGATE 400F

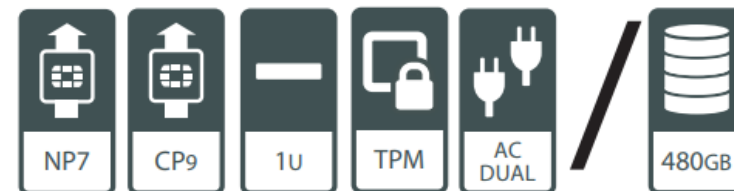
FortiGate 400F/401F



Interfaces

1. 1x USB Port
2. 1x Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 16x GE RJ45 Ports
5. 4x 1GE/10GE SFP+ Slots
6. 4x 10GE SFP+ Ultra Low Latency Slots
7. 8x 1GE SFP Slots

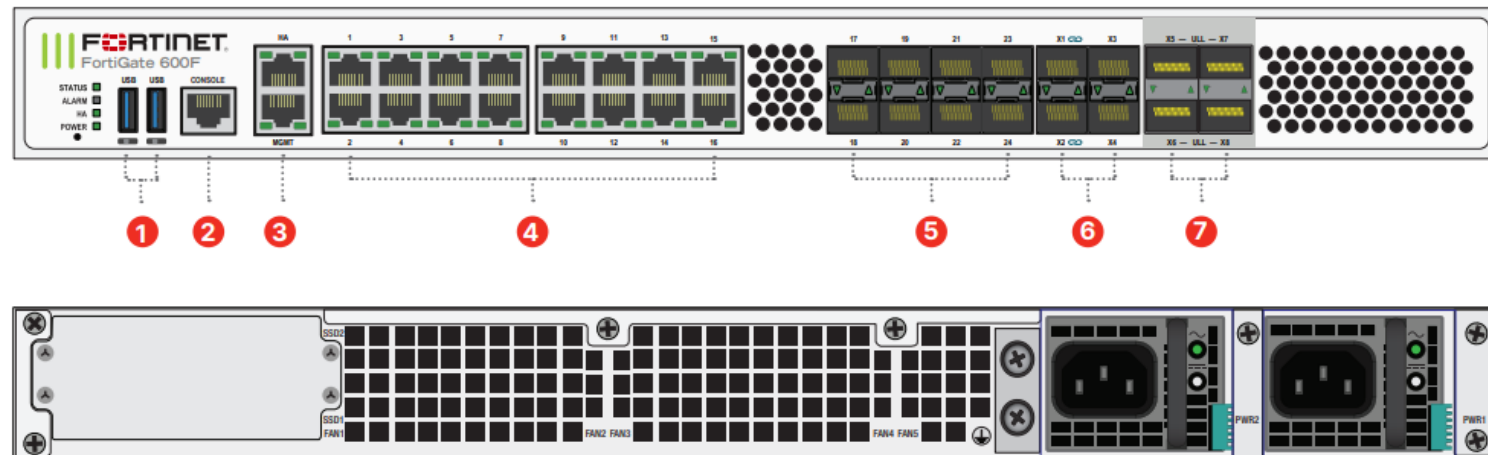
Hardware Features



Firewall*	IPS*	NGFW*	Threat Protection*
80 Gbps	10 Gbps	8 Gbps	6 Gbps

FORTIGATE 600F

FortiGate 600F/601F



Interfaces

1. 2x USB Ports
2. 1x Console Port
3. 2x GE RJ45 MGMT/HA Ports
4. 16x GE RJ45 Ports
5. 8x GE SFP Slots
6. 4x 10GE/GE SFP+/SFP Slots
7. 4x 25GE/10GE SFP28/SFP+ Ultra Low Latency Slots

Hardware Features



Firewall*

140 Gbps

IPS*

12 Gbps

NGFW*

9 Gbps

Threat Protection*

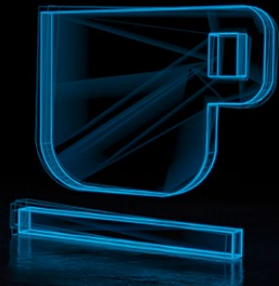
8 Gbps



FORTICARE – NEUE SUPPORT-STUFEN

ALSO & FORTINET

Tech & Snack



FORTICARE – NEUE SUPPORT-STUFEN

► FortiCare Essential

- Neuestes, billigeres FortiCare für tiefere FortiGate-Modelle (bis 80-Serie)
- Support beinhaltet lediglich WEB ONLY TICKETS und Chat, sowie Next-Business-Day-Response
- Kein Telefon-Support!

► FortiCare Premium

- Bisheriges 24x7 FortiCare mit FTS-Support, sowie 1h-Reaktion
- Service-Spektrum bleibt gleich

► FortiCare Elite

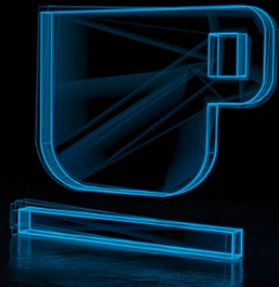
- Bisheriges ASE FortiCare mit FTS-Support, sowie 15min-Reaktion
- Breiteres Service-Spektrum
- Auch für FAP, FS, FAZ, FMG



FORTIOS 7.2 – NEUE FEATURES

ALSO & FORTINET

Tech & Snack



PLATFORM SUPPORT - FORTIOS 7.2.0

= zu einem späteren Zeitpunkt verfügbar, möglicherweise bei Patch-Veröffentlichungen
Grau = EoO-Produkte

	6.4.9	7.0.6	7.2
FG/FWF-60E	•	•	•
FG/FWF-40F Series	•	•	•
FG/FWF-60F Series	•	•	•
FG-80E Series	•	•	•
FG/FWF-80F Series	•	•	•
FG-90E Series	•	•	•
FG-100/101E Series	•	•	•
FG-100F Series	•	•	•
FG-200/201E	•	•	•
FG-200F	•	•	•
FG-300E/500E Series	•	•	•
FG-400E/600E Series	•	•	•
FG-800D/900D/1x00D Series	•	•	•

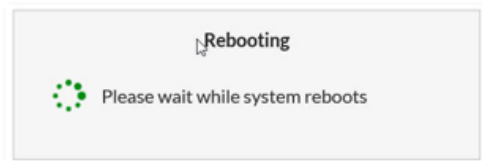
	6.4.9	7.0.6	7.2
FG-1100E Series	•	•	•
FG-1800F Series	•	#	#
FG-2200E, 3300E Series	•	•	•
FG-2000E, 2500E	•	•	•
FG-2600F Series	•	#	#
FG-3X00D Series (inc. 3800D)	•	•	•
FG-3810/3815D	•		
FG-3400E/3600E	•	•	•
FG-3500F series	•	#	#
FG-3960E/3980E	•	•	•
FG-4200/4400F Series	•	#	#
FG-5001D	•		
FG-5001E	•	•	•
FG-6000/7000 Series	•	#	#

DAS WISSEN WIR EIGENTLICH.... UPGRADEN

FORTIGATE UPGRADEN – VORBEREITUNG

FortiOS
6.4

- ▶ Software kann über das Supportportal von Fortinet heruntergeladen werden
- ▶ Release Notes durchlesen
- ▶ Upgrade Pfad unbedingt beachten
- ▶ Backup der Konfiguration erstellen
- ▶ Die FortiGate startet nach dem Upgrade neu



Select Product

FortiGate

Release Notes Download Upgrade Path FortiGate Support Tool

FortiOS Version Upgrade Path

Current Product: FortiGate-61F

Current FortiOS Version: 6.4.0 Upgrade To FortiOS Version: 6.4.6

Upgrade information for older FortiOS versions (before 5.2.9) can be found [here](#).

GO

Recommended Upgrade Path

Following is the recommended FortiOS migration path for your product.

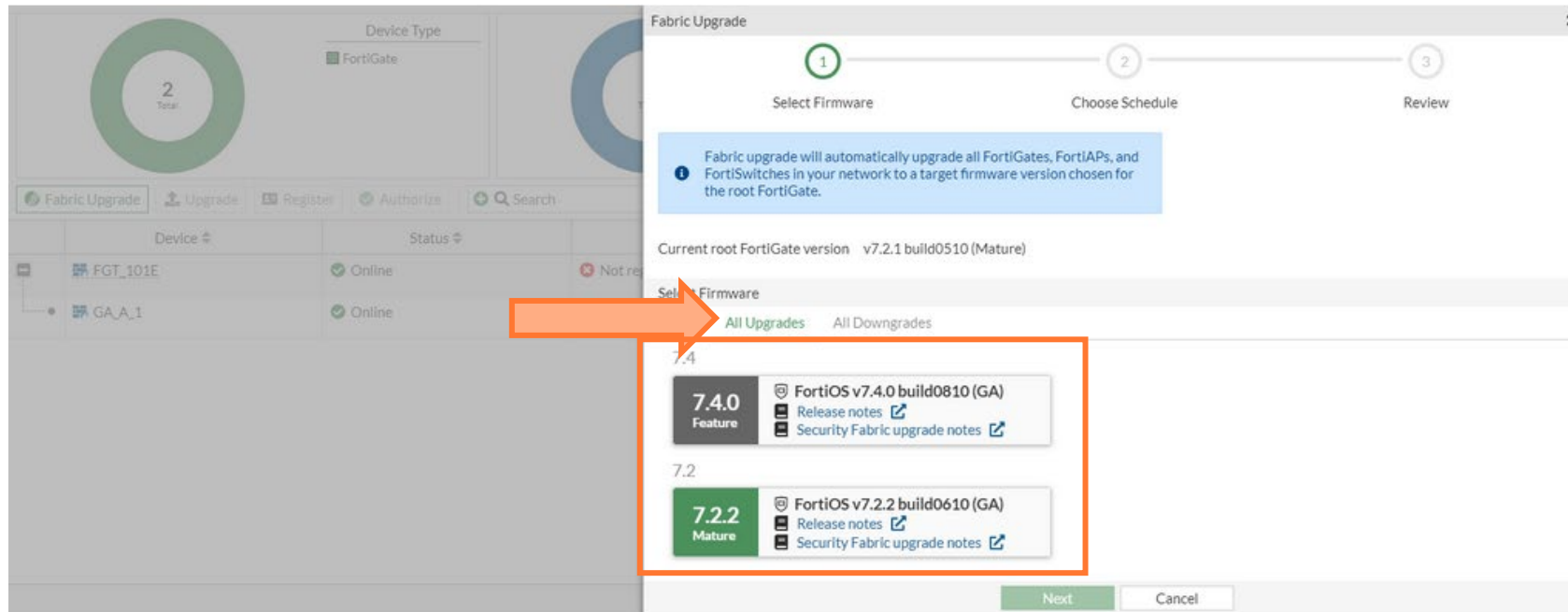
Version	Build Number
6.4.0	6025
6.4.2	1723
6.4.4	1803
6.4.6	1879

FOLLOW UPGRADE PATH

- ▶ Neue Option: Follow Upgrade path
 - ▶ Die Ziel-Firmware wird gemäss Upgrade-Path installiert, so dass Administratoren alle Upgrades einfach nacheinander durchführen können (mit mehreren Neustarts)
 - ▶ kann sofort oder zu einem geplanten Zeitpunkt durchgeführt werden

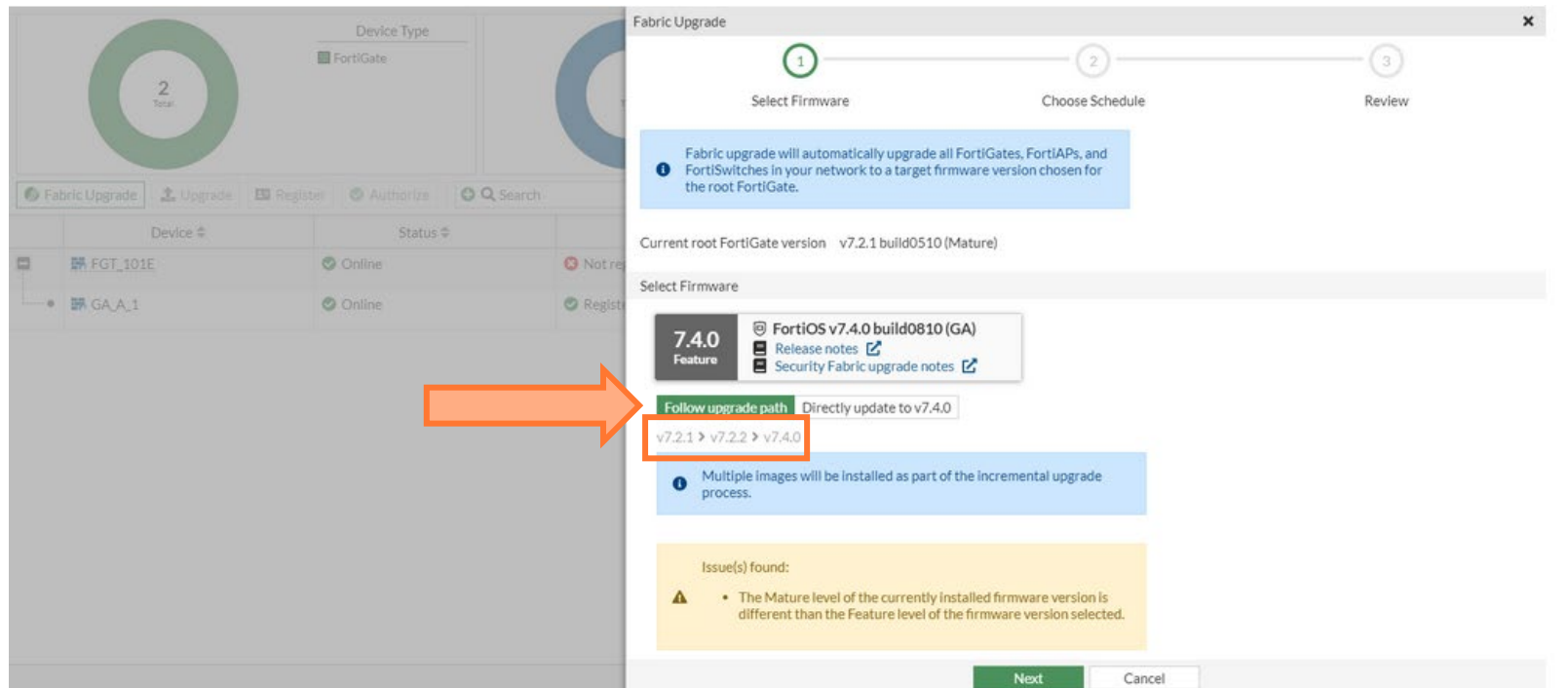
Device	Status	Registration Status	Firmware Version	Upgrade Status
FGT_101E	Online	Not registered	v7.2.1 build0510 (Mature)	v7.2.2 (Mature) available
GA_A_1	Online	Registered	v7.2.1 build0510 (Mature)	v7.2.2 (Mature) available

UPGRADE PATH – HOW TO...



1. Navigieren auf **System** → **Fabric Management** und auf **Fabric Upgrade** klicken. Der Bereich Fabric Upgrade wird geöffnet
2. Im Abschnitt **Select Firmware** die Option All **Upgrades** auswählen.

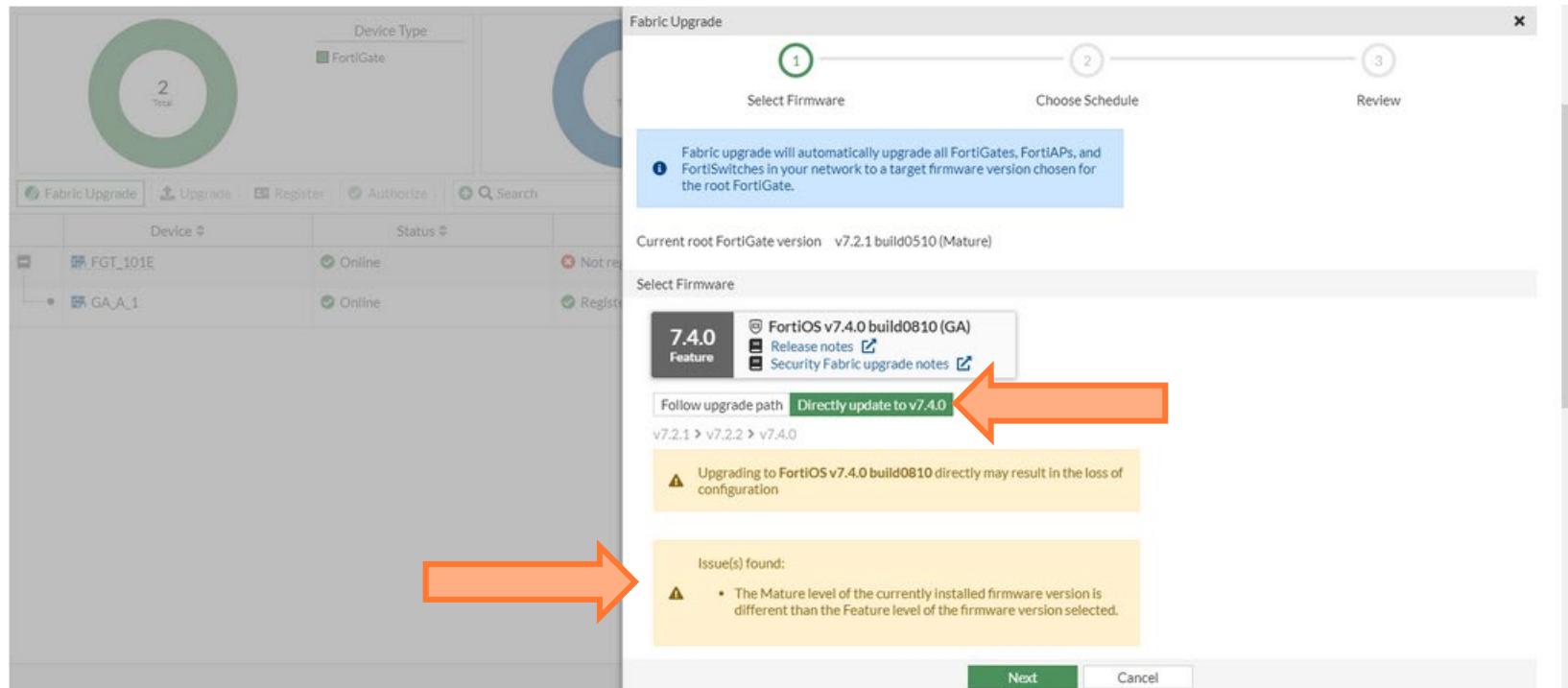
UPGRADE PATH – HOW TO...



3. Die Version **7.4.0** auswählen. Nun erscheinen die Upgrade Optionen

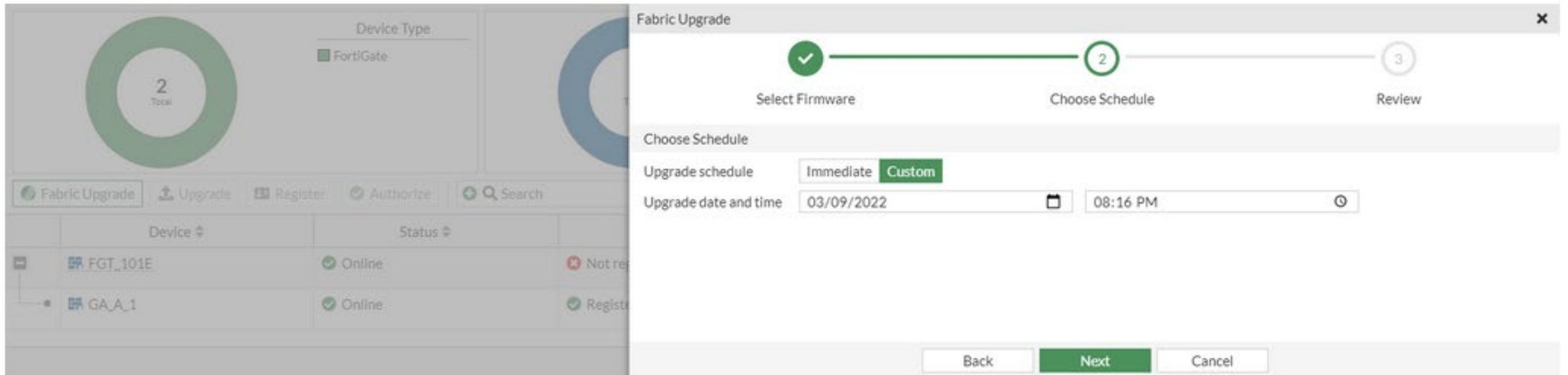
4. Die Option **Follow upgrade path**. Der Empfohlene Upgradepfad wird angezeigt: **v7.2.1 > v7.2.2 > v7.4.0**

UPGRADE PATH – HOW TO...



Wenn die **Directly upgrade to v7.4.0** gewählt wird, erscheint eine Warnmeldung, dass dies zu einem Verlust der Konfiguration führen kann

UPGRADE PATH – HOW TO...



5. Mit **Next** geht es weiter

6. Wahl des Upgrade-Zeitplan, entweder Sofort oder Benutzerdefiniert. Wenn man "Benutzerdefiniert" verwenden, das Datum und die Zeit für das Upgrade definieren (in diesem Beispiel wird "Benutzerdefiniert" verwendet).

UPGRADE PATH – HOW TO...

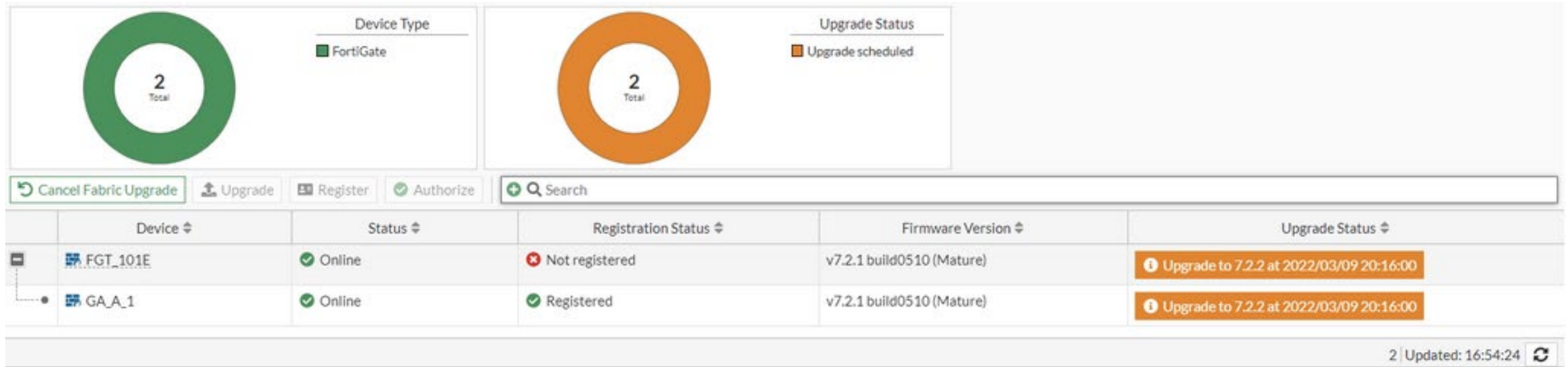
The screenshot displays the FortiGate Fabric Upgrade interface. On the left, a summary card shows '2 Total' devices. Below it, a table lists the devices: FGT_101E (Online) and GA_A_1 (Online). The main panel is titled 'Fabric Upgrade' and shows a progress bar with three steps: 'Select Firmware' (completed), 'Choose Schedule' (completed), and 'Review' (current step). Below the progress bar, a message states: 'Once confirmed, firmware versions will be upgraded as detailed below at 20:16 2022-03-09'. A table lists the upgrade details for each device:

Device	Firmware
FGT_101E	Upgrade to v7.4.0 (Feature) (2 steps)
GA_A_1	Upgrade to v7.4.0 (Feature) (2 steps)

At the bottom, there are three buttons: 'Back', 'Confirm and Backup Config' (highlighted in green), and 'Cancel'.

7. Nach dem anwählen von **Next** den Zeitplan noch einmal kontrollieren
8. Sobald **Confirm and Backup Config** angewählt wird, wird der Upgrade initiiert.

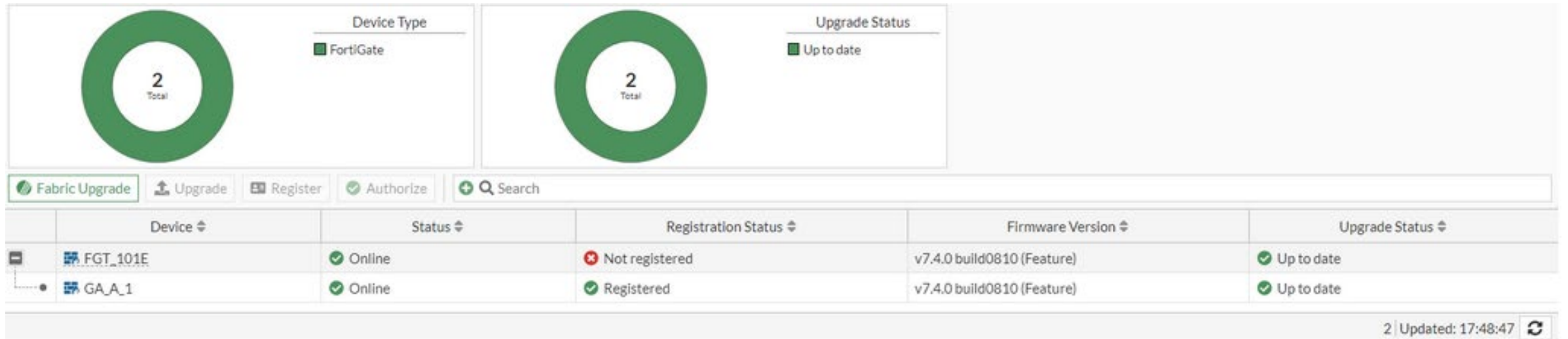
UPGRADE PATH – HOW TO...



Der Upgrade-Status für beide FortiGates zeigt an, wann das geplante Upgrade stattfinden wird. In diesem Beispiel ist das erste Upgrade im Pfad auf Version 7.2.2.

Die FortiGates werden neu gestartet und dann gemäss dem Upgrade-Pfad auf 7.4.0 aktualisiert

UPGRADE PATH – HOW TO...



Sobald die Upgrades abgeschlossen sind und auf beiden FortiGates die gewünschte Firmware (7.4.0) läuft, ändert sich der Upgrade-Status in Up to date.

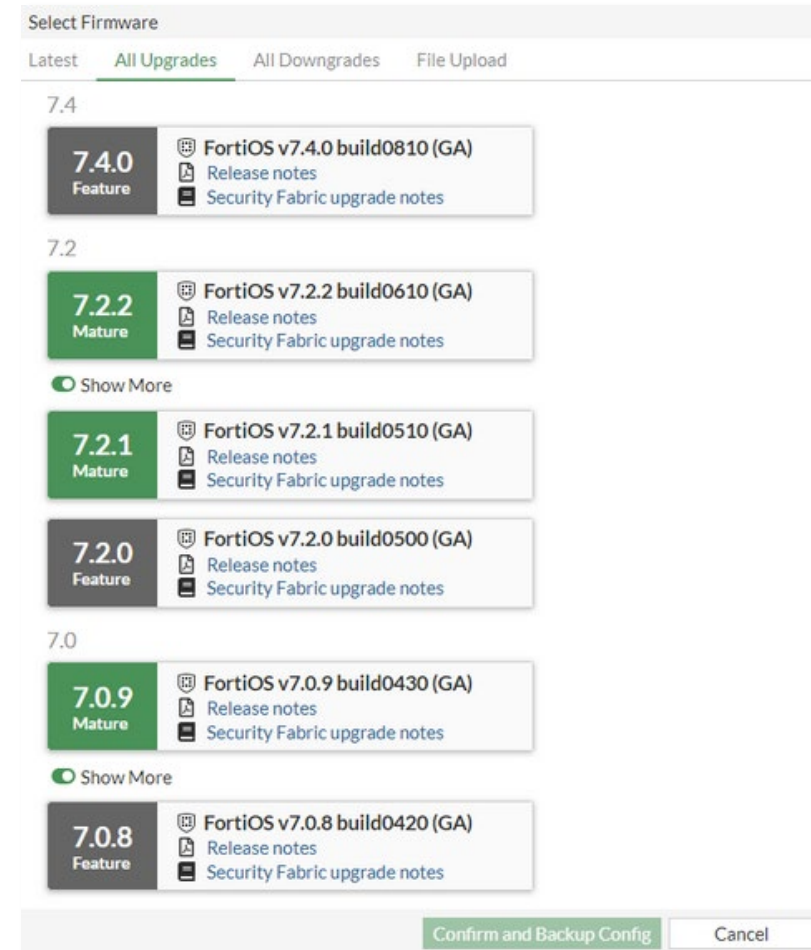
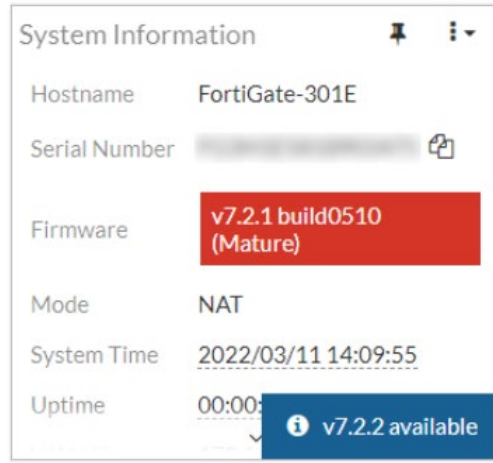
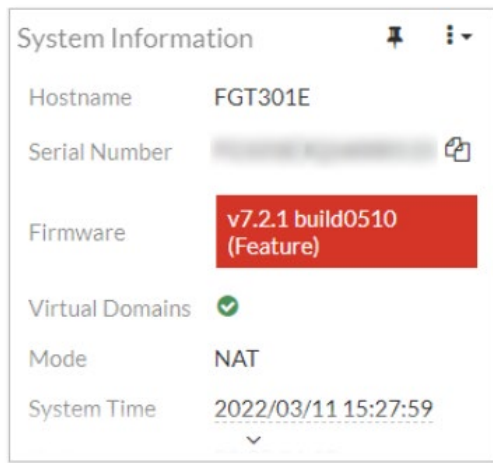
FIRMWARE LEVEL ERSICHTLICH

► Feature Release:

- Neue Features oder CLI Änderungen im Release enthalten.

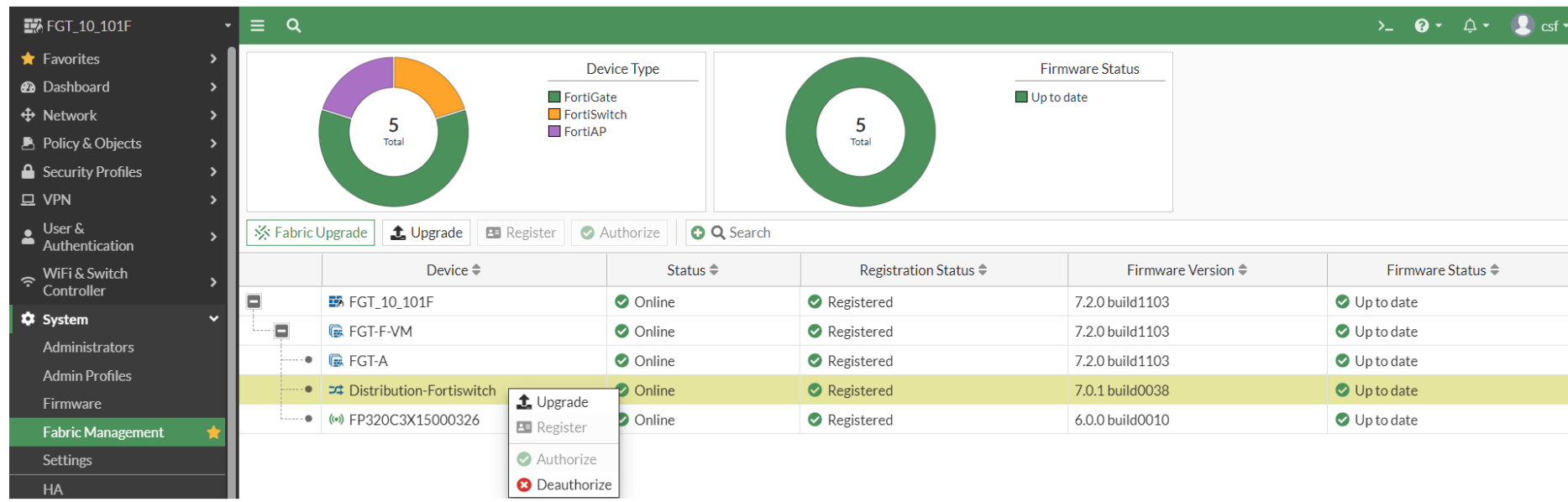
► Mature Release:

- Keine neuen Features oder CLI Änderungen im Release enthalten



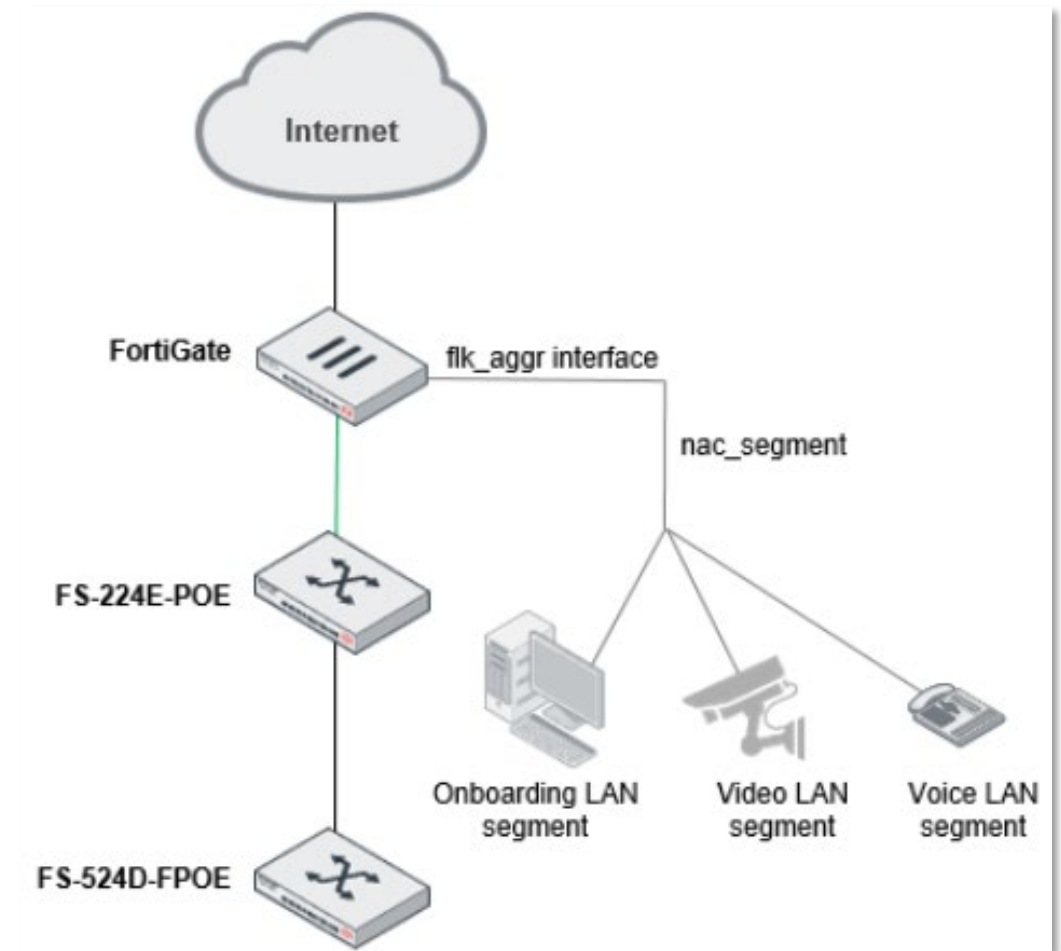
DEVICE MANAGEMENT

- ▶ Neue Fabric-Geräteübersichtsseite zur Auflistung von Fabric-Netzwerkgeräten
 - ▶ Aufgelistete Geräte - FG, FSW, FAP und FEX
 - ▶ Zentralisierte Statusanzeige, Firmware-Verwaltung, FortiCare-Registrierung und -Autorisierung



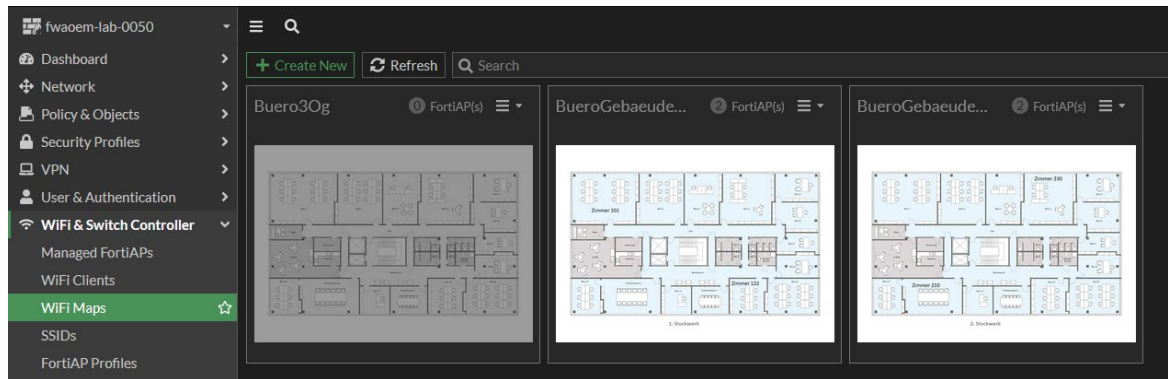
LAN SEGMENTATION GUI

- ▶ Hinzufügen von GUI-Konfiguration und Verbesserungen an der NAC-LAN-Segmentierungsfunktion
- ▶ Anzeige von NAC-Segment- und LAN-Segment-VLANs als Parent- und Child-VLANs auf der **Network → Interface** Seite
- ▶ Hinzufügen eines VLAN-Segment-Toggles, um die VLAN-Segmentierung auf einem Switch-VLAN-Interface anzuwenden
- ▶ Hinzufügen eines NAC-Einstellungsdialogs zur NAC-Policy Seite, um NAC VLAN zu aktivieren und die primären, Onboarding- und Segment-VLANs zu ändern

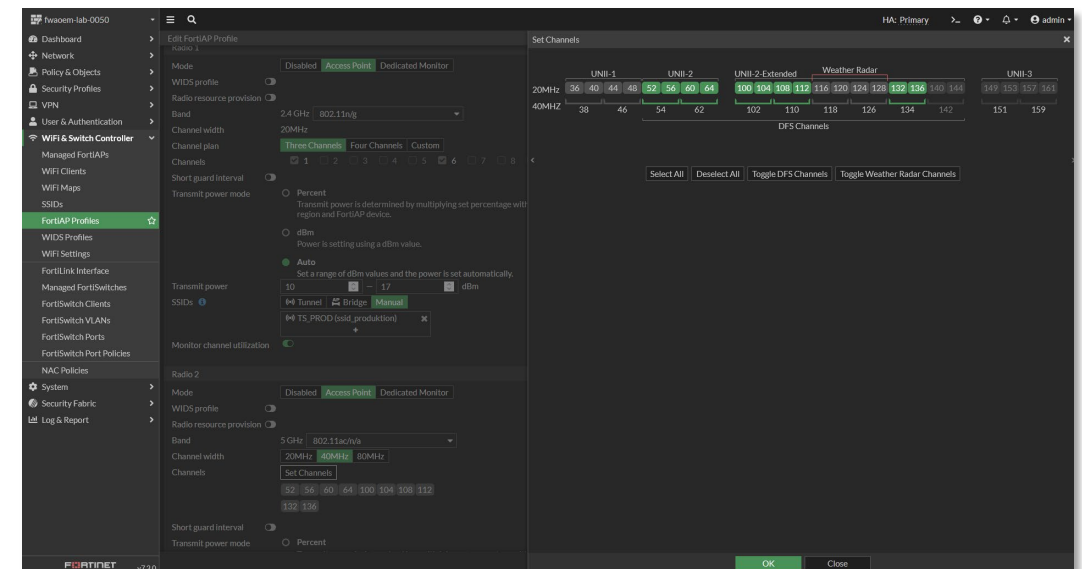


WIFI FEATURES - ZUSAMMENGEFASST

- Mehrere WiFi Karten einlesen:



- Verbesserte WiFi-Kanalauswahl im GUI:




Alle Features im Wireless Bereich:

<https://docs.fortinet.com/document/fortigate/7.2.0/new-features/937037/wireless>


ISDB – IP ADRESSEN LOOKUP

- ▶ IP Adressen Lookup in ISDB-Objekten
 - ▶ IP-Informationen aus der ISDB und GeoIP Datenbank abrufen
- ▶ Die zurückgegebenen IP-Adressinformationen umfassen folgende Angaben:
 - ▶ Reverse IP-Adresse
 - ▶ Reverse Domain Lookup
 - ▶ Standort,
 - ▶ Reputation
 - ▶ andere Internetdienstinformationen.

 IP Address Lookup

IP Address Query

IP Address Details

IP Address	 8.8.8.8
Owner	Google
Location	Mountain View, California, United States
Coordinates	37.386051 / -122.083847
Reputation	Unverified site
Popularity	★★★★★

Internet Service Details

ID	Reputation	Popularity
DNS-DoH_DoT	Unverified site	★★★★☆
Google-Web	Reputable site from social media	★★★★★
Google-ICMP		
Google-DNS		
Google-Outbound_Email		
Google-SSH		
Google-FTP		
Google-NTP		
Google-Inbound_Email		
Google-LDAP		

<https://docs.fortinet.com/document/fortigate/7.2.0/new-features/635185/look-up-ip-address-information-from-the-internet-service-database-page>

GRAFISCHE DIAGNOSTIK TOOLS

Debug Flow Seite

- ▶ GUI-Unterstützung für den Debug-Flow von Paketen
- ▶ Tabellarische und Userfreundliche Ausgabe

Eingebaute Echtzeit Paketaufzeichnungs- und Analysewerkzeug

- ▶ Paketerfassung kann direkt von dem WebGUI aus untersucht werden
- ▶ Beseitigt die Notwendigkeit der Verwendung von Drittanbieter-Viewern wie Wireshark

The screenshot displays the FortiGate WebGUI interface. On the left is a navigation menu with categories like Network, Diagnostics, and Policy & Objects. The main area is divided into two panels. The top panel, titled 'Debug Flow', shows a list of packet processing events with columns for Time, Message, and Function. The bottom panel, titled 'Packet Capture', shows a table of captured packets with columns for Time, Source IP, Destination IP, Source Port, Destination Port, and Protocol. Below the table is a 'Packet Data' section showing the raw packet data in hexadecimal and ASCII. A 'Filter' sidebar is visible on the right of the Debug Flow panel.

Time	Message	Function
18:16:54	vd-root:0 received a packet(proto=1, 172.16.151.87:768->4.2.2.1:2048) tun_id=0.0.0.0 from local, type=8, code=0, id=768, seq=0	print_pkt_detail
18:16:54	allocate a new session-0000f417, tun_id=0.0.0.0	init_ip_session_common
18:16:54	in[], out-[port1]	iprope_dnat_check
18:16:54	len=0	iprope_dnat_tree_check
18:16:54	result: skb_flags-00000000, vid-0, ret-no-match, act-accept, flag-00000000	iprope_dnat_check
18:16:54	gnum-100004, check-fffffffa00432d0	iprope_check
18:16:54	checked gnum-100004 policy-1, ret-no-match, act-drop	iprope_check_one_policy

Time	Source IP	Destination IP	Source Port	Destination Port	Protocol
0.07541s	172.16.200.254	172.16.200.1	55897	443	TCP
1.06700s	172.16.200.254	172.16.200.1	55897	443	TCP
2.04962s	172.16.200.254	172.16.200.1	53799	443	TCP
2.05034s	172.16.200.254	172.16.200.1	53799	443	TCP
2.05063s	172.16.200.254	172.16.200.1	53799	443	TCP
2.05555s	172.16.200.254	172.16.200.1	53799	443	TCP
2.05653s	172.16.200.254	172.16.200.1	53799	443	TCP

ARTIKEL DIAGNOSE FEATURES / ISDB LOOKUP

▶ Debug Flow

- ▶ <https://docs.fortinet.com/document/fortigate/7.2.0/new-features/462154/embed-real-time-packet-capture-and-analysis-tool-on-diagnostics-page>
- ▶ <https://docs.fortinet.com/document/fortigate/7.2.0/new-features/38044/embed-real-time-debug-flow-tool-on-diagnostics-page>

▶ Paket Capture/Sniffer:

- ▶ <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Debug-flow-tool/ta-p/213238>
- ▶ <https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-run-a-real-time-Wireshark-capture-on/ta-p/213805>

▶ ISDB Lookup

- ▶ <https://docs.fortinet.com/document/fortigate/7.2.0/new-features/635185/look-up-ip-address-information-from-the-internet-service-database-page>

WORKFLOW MANAGEMENT

Policy Change Summary

- ▶ Zusammenfassung von Policy Änderungen
- ▶ Bei Policy Änderungen erscheint ein Comment-Feld für den Administrator zur Eingabe von etwaigen Kommentaren.
- ▶ Optionen wie "immer erforderlich" und "optional"
- ▶ Admin kann Audit Trail für eine Firewall-Regel anzeigen

The screenshot displays the 'Workflow Management - Summarize Changes' window in FortiManager. It shows a summary of changes for a policy named 'DMZ-INET'. The interface includes a sidebar with various configuration options like Firewall/Network Options, Security Profile, and Audit trail for Firewall. The main area contains a 'Workflow Management' section with settings for 'Configuration save mode' (Automatic), 'Policy change summary' (Required), and 'Policies expire by default' (30 Days). Below this is a table showing a list of changes with columns for Date, Action, and User. At the bottom, there is a 'Changes' table with columns for Attribute, Previous Value, and New Value, and a 'Metadata' section with fields like Date, Action, Summary, Changed by, and Transaction ID.

Workflow Management - Summarize Changes

A change summary is required due to Workflow Management settings. The summary used here can be referred back to for auditing purposes.

Object: DMZ-INET

Change summary: [Text Field]

Workflow Management

Configuration save mode: **Automatic** | Workspace

Policy change summary: **Required** | Optional

Policies expire by default: ☒ **Expire after**: 30 Days

Date	Action	User
14/03/2022 12:23:07	test	admin
14/03/2022 11:49:38		admin
14/03/2022 11:47:58		admin
14/03/2022 11:32:01		admin
14/03/2022 11:27:06		admin
14/03/2022 11:25:37		admin

54% 22 | Updated: 15:30:56

Attribute	Previous Value	New Value
policy-expiry-date	2022-03-24 12:22:34	2022-03-31 12:22:00

Metadata

Date	14/03/2022 12:23:07
Action	Edit
Summary	change expire date
Changed by	admin
Transaction ID	11731021

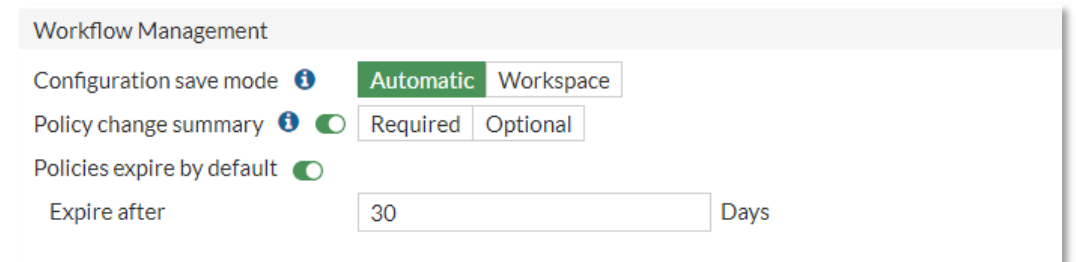
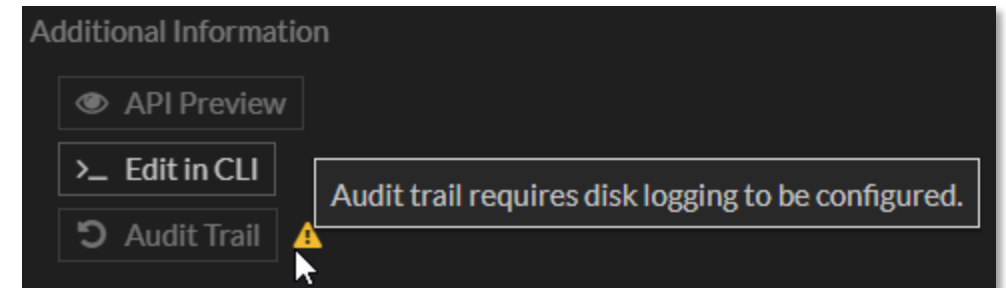
WORKFLOW MANAGEMENT

► Policy Change Dokumentation

- Kommentar bei jeder Firewall-Regel
- Änderung kann Optional oder Erzwungen werden
- Um die Audit Logs zu sehen ist eine Disk notwendig

► Gültigkeit der Firewall Regeln


- Wenn diese Funktion für eine Firewall Regel aktiviert wird, kann der Administrator den Zeitpunkt für das Auslaufen der Policy definieren(default Wert ist 30 Tage)
- Der Wert kann selber definiert werden.



SECURITY FABRIC | AUTOMATION STITCHES

- ▶ Neue Automation Trigger
- ▶ Es wurden sechs neue Trigger hinzugefügt, welche auf verschiedenen **Eventlog Kategorien** basieren:
 - ▶ **Anomaly Logs**
 - ▶ **SSH Logs**
 - ▶ **Virus Logs**
 - ▶ **IPS Logs**
 - ▶ **Traffic Violation**
 - ▶ **Webfilter Violation**

Create New Automation Trigger







 **Virus Logs** A virus event has occurred.

Name

Description

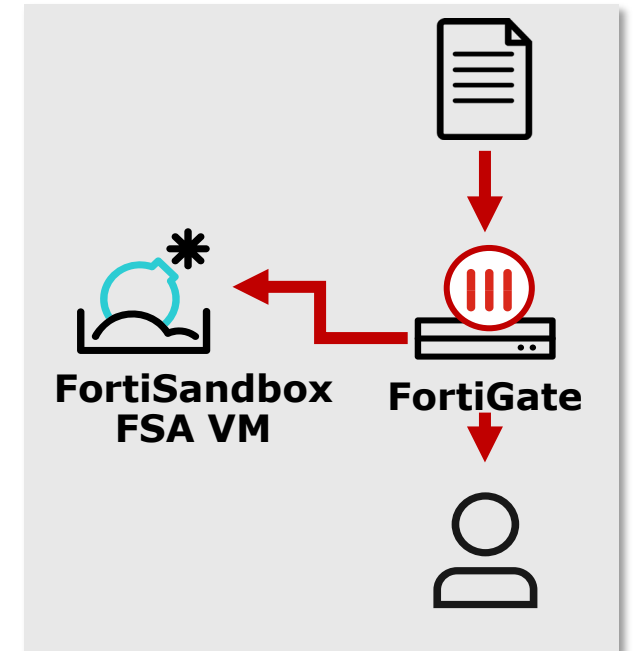
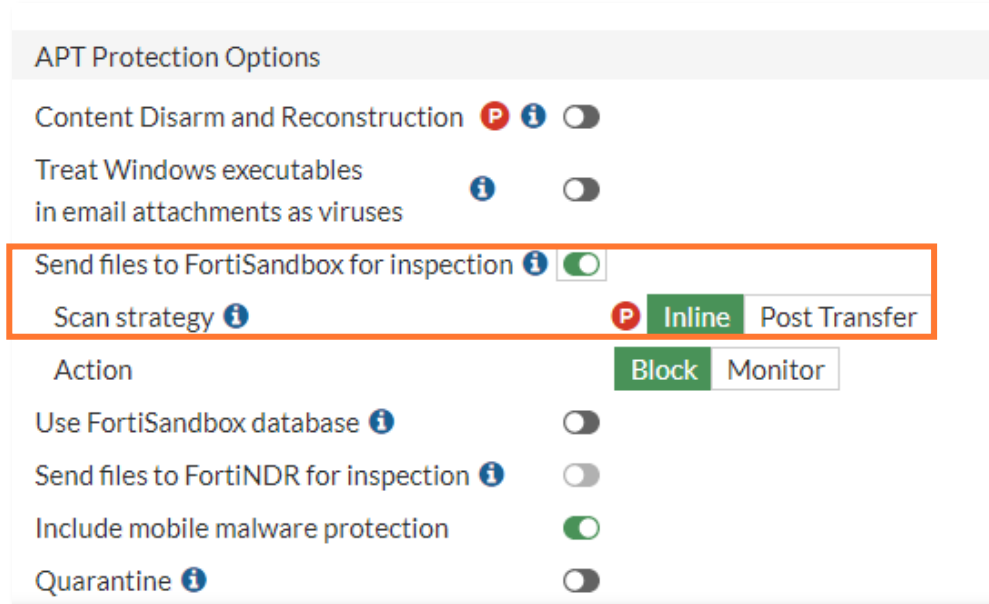
0/255

Event Log Category

 Anomaly Logs An anomalous event has occurred.	 IPS Logs An IPS event has occurred.
 SSH Logs An SSH event has occurred.	 Traffic Violation A traffic policy has been violated.
 Virus Logs A virus event has occurred.	 Webfilter Violation A webfilter policy has been violated.

FORTISANDBOX INLINE SCANNING

- ▶ Unterstützung von Hold-&-Release für von FortiSandbox untersuchte Dateien
 - ▶ FGT kann so konfiguriert werden, dass es auf das FSA-Ergebnis wartet, bevor die Datei an das Ziel freigegeben wird.
 - ▶ Administratoren können künstlich erzeugte Verzögerung konfigurieren, um das teilweise oder endgültige, bekannte Ergebnis der FSA abzuwarten
- ▶ Verwendet HTTP2 (Streaming), damit die FGT den Download sowohl an die FSA als auch an den Endbenutzer weiterleitet und nur die letzten Pakete zurückhält



KONFIGURATION ÜBER DIE CLI

► FortiSandbox inline scanning aktivieren:

```
config system fortisandbox
  set status enable
  set inline-scan {enable | disable}
  set server <fortisandbox_server_ip>
end
```

► Konfiguration FortiSandbox scanning Optionen im Antivirus Profil:

```
config antivirus profile
  edit <name>
    set fortisandbox-mode {inline | analytics-suspicious | analytics-everything}
    set fortisandbox-error-action {ignore | log-only | block}
    set fortisandbox-timeout-action {ignore | log-only | block}
    set fortisandbox-max-upload <integer>
    config {http | ftp | imap | pop3 | smtp | mapi | cifs | ssh}
      set av-scan {disable | block | monitor}
      set fortisandbox {disable | block | monitor}
    end
  next
end
```

<https://docs.fortinet.com/document/fortigate/7.2.0/new-features/571153/fortisandbox-inline-scanning>

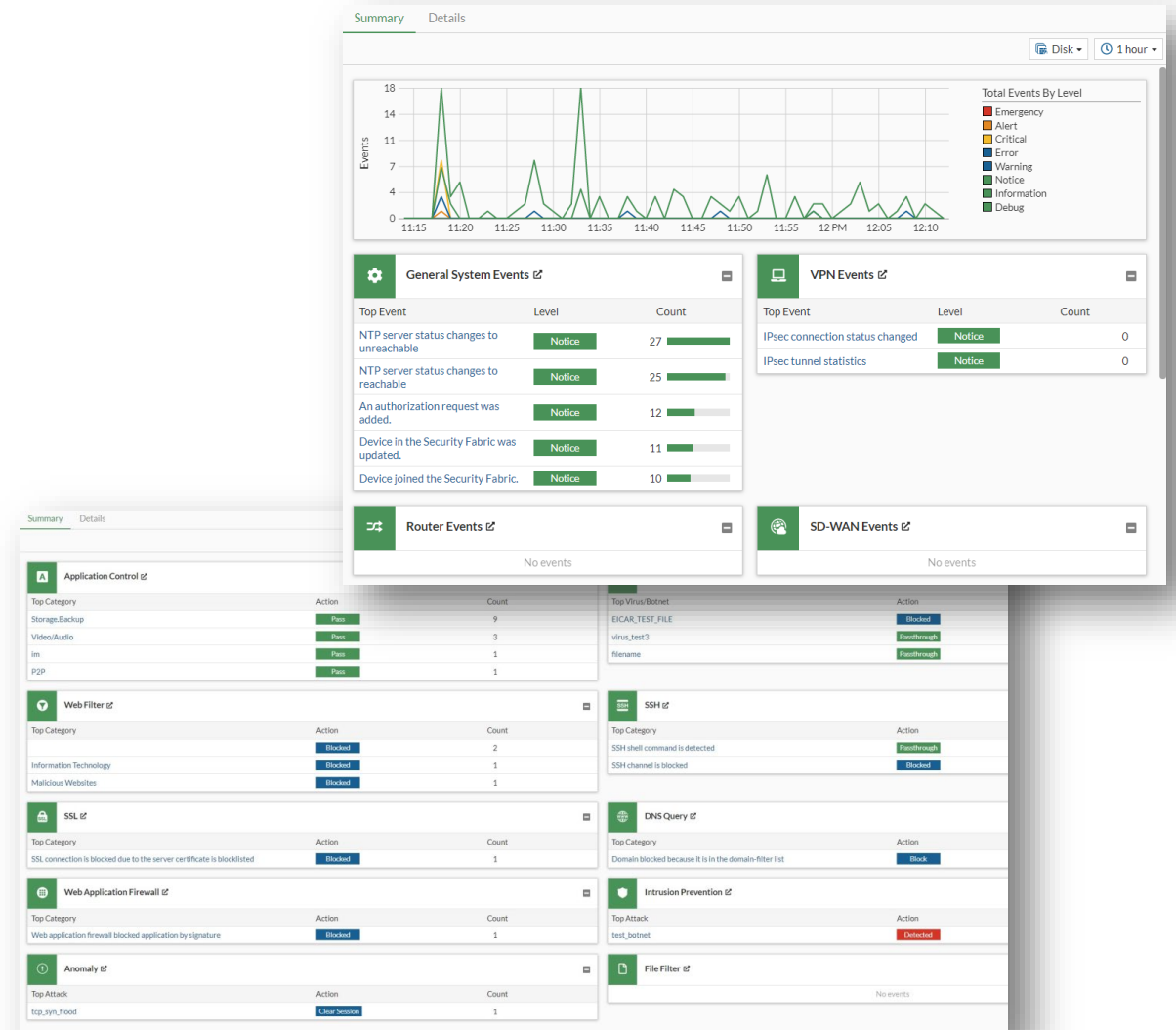
ÜBERARBEITETE LOG SEITEN – SYSTEM EVENTS

► System Event Log Seite

- Enthält eine neue Registerkarte "Zusammenfassung"
- Durch Anklicken eines Ereignisses auf der Registerkarte "Zusammenfassung" gelangt der Benutzer automatisch zur Registerkarte "Details" mit den entsprechenden Filtern

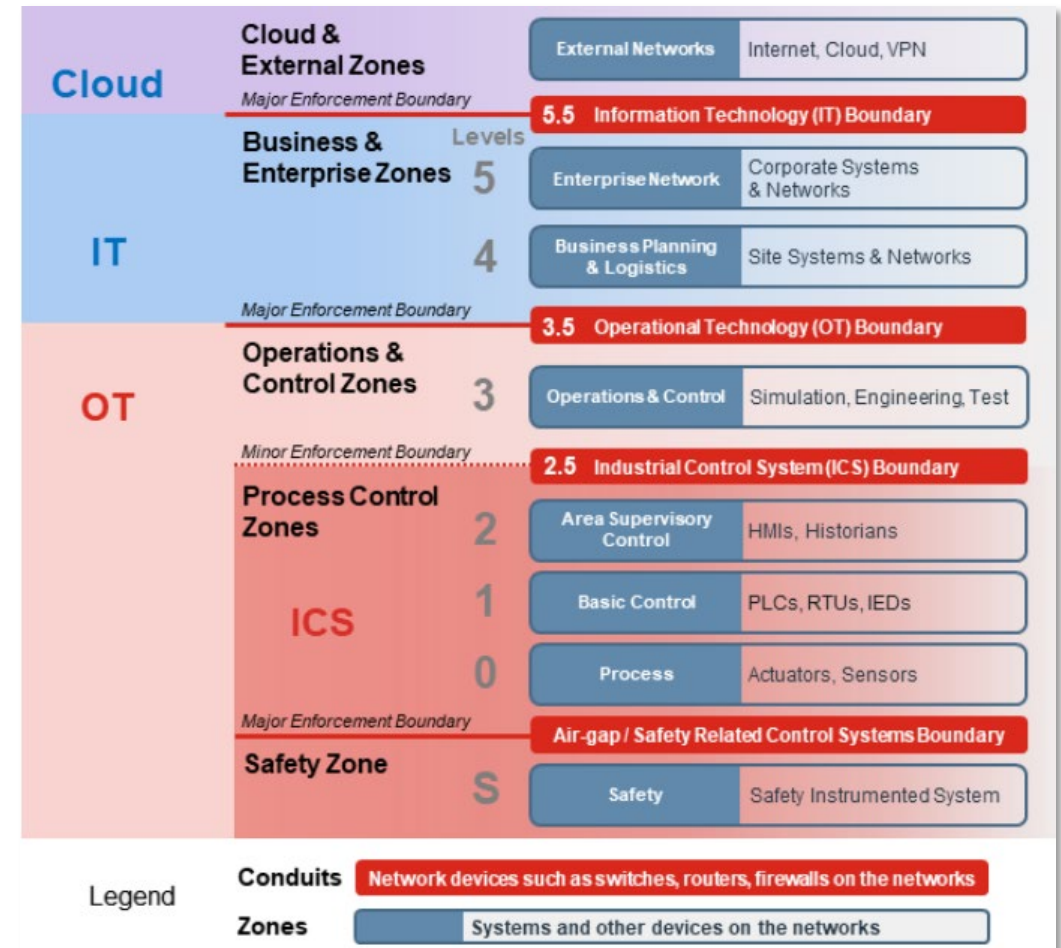
► Security Log Seite

- UTM-Protokoll-Subtypen sind jetzt kombiniert
- Zugang zu interessierenden Logs über die neue Zusammenfassungsseite

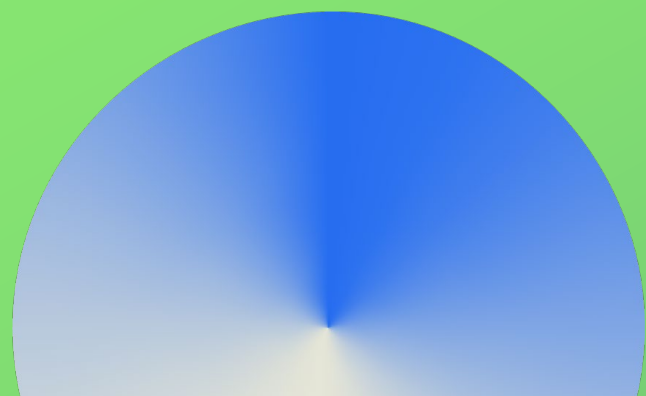


OT ASSET VISIBILITY

- ▶ Voraussetzung: IoT detection service subscription
- ▶ Grafische Übersicht der OT/IoT Devices
- ▶ Devices lassen sich via drag'n drop in die verschiedenen Purdue Level ziehen
- ▶ Purdue Enterprise Reference Architecture ist ein Referenzmodell für Unternehmensarchitektur aus den 1990er Jahren, das von Theodore J. Williams und Mitgliedern des Industry-Purdue University Consortium for Computer Integrated Manufacturing entwickelt wurde. [Wikipedia \(Englisch\)](https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture)



<https://docs.fortinet.com/document/fortigate/7.2.0/new-features/498242/add-ot-asset-visibility-and-network-topology-to-asset-identity-center-page>

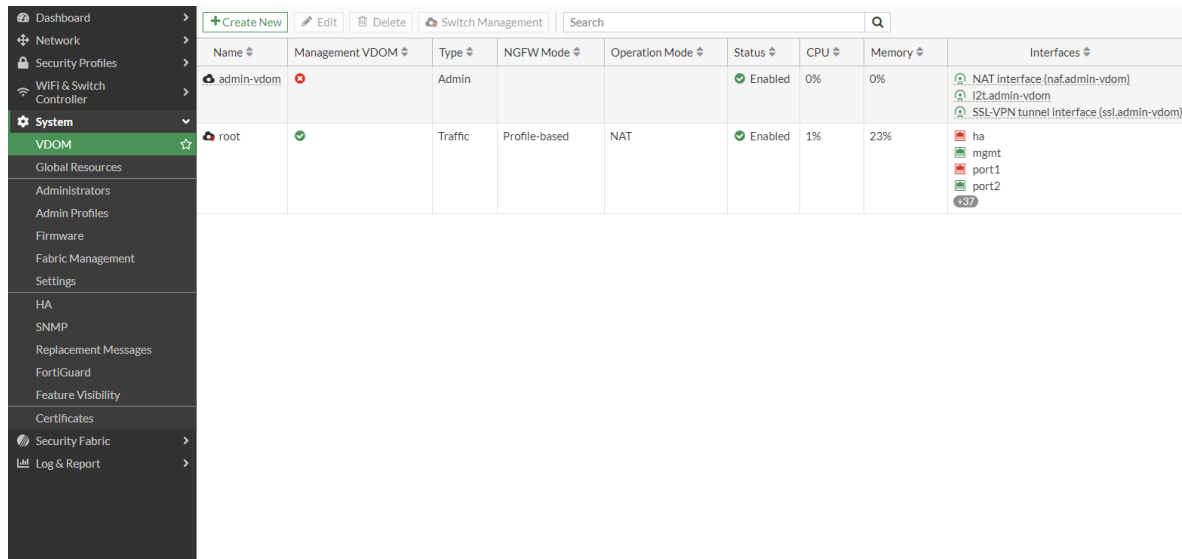


DEMO OT VIEW



VDOM - TYPEN

- ▶ Organisieren von VDOMs für bestimmte Zwecke
 - ▶ 2 VDOM-Typen = Traffic, Admin(Management)
 - ▶ Admin-VDOM ersetzt den Split-Task-VDOM-Modus



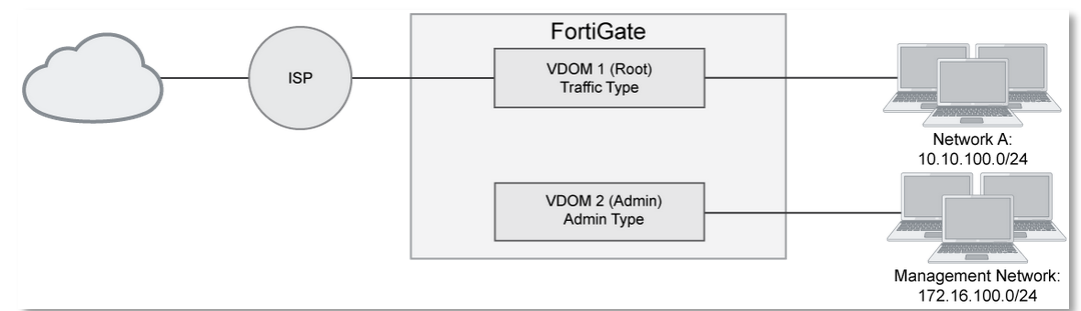
Name	Management VDOM	Type	NGFW Mode	Operation Mode	Status	CPU	Memory	Interfaces
admin-vdom		Admin			Enabled	0%	0%	NAT interface (naf.admin-vdom) l2tadmin-vdom SSL-VPN tunnel interface (ssl.admin-vdom)
root	✓	Traffic	Profile-based	NAT	Enabled	1%	23%	ha mgmt port1 port2

- ▶ VDOM Mode aktivieren:

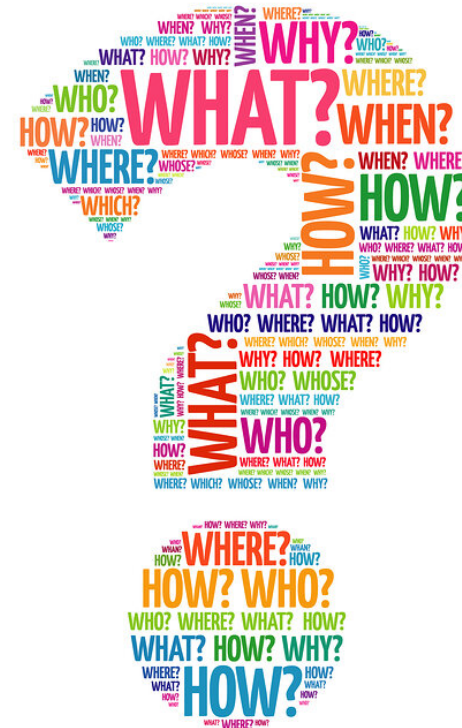
```
config system global
    set vdom-mode multi-vdom
end
```

- ▶ VDOM Typ definieren:

```
config system settings
    set vdom-type {traffic | admin}
end
```



Q&A



Gerne stehen wir euch nun für Fragen und Anregungen zur Verfügung.
Fragen gerne an fortinet-ch@also.com
Besucht auch <https://fortinet.also.ch/wiki>

THANK YOU

